A. Pre-CALEA Electronic Surveillance

7. For many decades, law enforcement agencies have been able to employ court-ordered electronic surveillance successfully in collecting evidence in criminal investigations. The principal statutory authority allowing these agencies to conduct electronic surveillance is contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (hereinafter "Title III"), as amended by the Electronic Communications Privacy Act of 1986 ("ECPA") (codified at 18 U.S.C. §§ 2510 et seq.). In 1986, Congress modified Title III in order to update its provisions and clarify federal privacy protections and electronic surveillance standards in light of changes in computer and telecommunications technologies. In addition, Congress added a court order requirement for "pen registers" and "trap and trace" devices. (18 U.S.C. §§ 3121 et seq.).[2] ("Pen registers" do not intercept the contents of calls, but instead record outgoing dialed digits, tones, and any other signals from a subscriber's telecommunications equipment or facilities; "trap and trace" devices provide information concerning the origination of incoming calls.)

8. Title III imposes significant responsibilities on law enforcement officers in order to protect privacy to the maximum extent possible while allowing evidence gathering through electronic surveillance. For example, a law enforcement agency is obligated to demonstrate that other practical investigative techniques are unavailing before seeking electronic surveillance authorization (18

---

[2] The history of federal wiretap legislation is described in the Commission's Notice of Proposed Rulemaking in In the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, FCC 97-356 (released Oct. 10, 1997), at 4-8 (cited hereafter as "FCC Notice").

U.S.C. § 2518(3)(c)), and it must minimize interception of non-criminal conversations (18 U.S.C. § 2518(5)). In addition, tapes of intercepted communications must be sealed at the end of the interception period (18 U.S.C. § 2518(8)), and only authorized disclosures of such material are permitted (18 U.S.C. §§ 2511(1)(c) and 2517).

9. Law enforcement agencies have often conducted electronic surveillance with the assistance of the telecommunications industry, but sometimes have been forced to proceed without the industry's cooperation. In some instances, certain service providers have refused to render needed assistance to law enforcement officers even when surveillance was judicially authorized. See, e.g., Application of United States, 427 F.2d 639 (9th Cir. 1970). In light of this problem, in 1970, Congress amended Title III to make clear the responsibility of telephone service providers to provide assistance to law enforcement personnel. Specifically, Congress amended Title III to provide that interception orders shall "direct that a provider of wire or electronic communication service * * * shall furnish the applicant [for the order] forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider * * * is according the person whose communications are to be intercepted." 18 U.S.C. § 2518(4).

10. Despite the 1970 amendments to Title III, telephone service providers have continued in certain instances to refuse full cooperation for criminal investigations, forcing law enforcement officials to seek compulsion from the courts. See, e.g., United States v. New York Telephone Co., 434 U.S. 159 (1977) (compelling telephone company to provide assistance to the FBI in installing

pen registers); United States v. Mountain States Telephone and Telegraph Co., 616 F.2d 1122 (9th Cir. 1980) (compelling telephone company to program computerized electronic switching equipment so that the IRS could determine numbers from which incoming calls to target were being made); Michigan Bell Telephone Co. v. United States, 565 F.2d 385 (6th Cir. 1977) (compelling telephone company to employ both manual and electronic tracing devices on specified telephones).

11. Prior to 1984, the great majority of local and long distance telecommunications were carried by AT&T, which held a virtual monopoly on these services. This dominance resulted in a largely homogeneous telephone network in which the technology of the equipment used to conduct business was generally uniform throughout the network. The telephone system was largely based on "analog" technology, which converted voices into electronic patterns that mimic natural sound waves. The electronic impulses would then travel over copper wires, and were directed to the receiver by electronic contact switches. Law enforcement agents were consistently able to conduct electronic surveillance by gaining access to telephone lines between the service provider's central office and a telephone subscriber's home or office (the "local wire loop"). These interceptions were highly effective for the existing technologies, and law enforcement agents were able to intercept the content of all communications supported by a subscriber's service or carried over the subscriber's facilities, as well as information concerning the nature of any calls (such as from which numbers they came and to which numbers they went). In addition, these agents could verify the accuracy, integrity, and operability of the surveillance throughout the interception period.

12. Thus, until fairly recently, law enforcement officers could obtain all information available to the telephone service provider concerning use of the services that it rendered to a particular subscriber, including when and to which numbers calls were made, when and from which numbers calls were received, and the complete contents of those calls. In other words, everything then technologically possible to know about the telephone service being provided was available to authorized law enforcement officers. Further, there were no technological limitations on the number of interceptions that could be conducted.

13. This situation changed considerably and rapidly in the past 20 years, particularly following the breakup of AT&T in 1984. The number of long distance and local service providers has increased dramatically, and this number has expanded even further with the advent of wireless technologies. Law enforcement agencies must now deal with well over one thousand different telecommunications service providers who are employing a host of new technological developments. These developments are possible in part because analog technology is being replaced by digital technology, under which a communication is converted by computer into streams of binary data representing the digits "0" and "1". Rather than being routed by an electrical contact switch, a call is typically routed by a computer at the carrier's switching facility.

14. As this petition indicates, the development of new telecommunications technologies has provided subscribers with a range of new services that enable them to accomplish tasks with their telephone systems that could not be done before. For example, in the past decade or so, the following services became widely available to subscribers: call forwarding; call transferring; direct

implementation by a subscriber of new services: voice-activated dialing and speed dialing from the service provider's centralized facility; the ability to have voice "mail box" message systems accessed by a subscriber; and the ability to initiate a multi-party call and then depart, leaving the other parties still connected.

15. These new telecommunications technologies allow for the efficient transmission of multiple, simultaneous communications of various subscribers over fiber optic lines and wire facilities. Features such as call forwarding permit customers to redirect calls, thereby no longer requiring that communications be transmitted to the same specific location or through the same wire line loop. Likewise, "follow me" features expand the nature of call forwarding to national dimensions. And personal communications services enable users to define their own set of subscribed services, use any fixed or mobile terminal or telephone instrument, and make and receive calls across multiple networks without regard to their location. All of these services have removed a telephone subscriber from a fixed local wire loop that could be tapped by law enforcement agents, and thereby have greatly hampered the ability to conduct court approved electronic surveillance. See also FCC Notice at 10 ("In addition to the proliferation of services currently offered, the increase in the sheer number of service providers further complicates efforts to conduct the authorized implementation of electronic surveillance").

16. Moreover, as new technology is deployed, the principal technique used for electronic surveillance of telecommunications will also change. In the past, law enforcement officers typically utilized their own equipment physically to tap into an existing wire leading to a subscriber's house

or business. However, with the advent of digital transmissions and the use of a telecommunications carrier's computer to provide services at a centralized point, electronic surveillance will often be accomplished through the use of software employed by the carrier to route authorized information to law enforcement officers.

B. The Enactment of CALEA

17. In March 1994, FBI Director Freeh informed Congress that the telecommunications technological revolution was having a devastating impact on the ability of law enforcement officers to carry out their essential electronic surveillance duties. See Joint Hearings on Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House of Representatives Comm. on the Judiciary, 103d Cong., 2d Sess. 5-6, 14 (March 18, 1994) (statement of Louis J. Freeh). Director Freeh explained to Congress that "[i]ndustry representatives have bluntly told law enforcement that the existing telecommunications systems and networks will thwart court authorized intercepts" (id. at 24). The developments in telecommunications technology "often prevent, and will continue to prevent common carriers from providing law enforcement with access to all of the communications and dialing information that are the subject of electronic surveillance and pen register court orders" (id. at 24). The telecommunications industry had been telling the FBI that "there is a serious problem, and they have been forecasting that within a very short period of time they will not be able to service

our court orders" (id. at 9); "they will not have in the switches the software necessary to make the connections to give us the access" (id. at 10).

18. In addition, based on a survey, Director Freeh pointed out that it was estimated that in the prior decade several hundred electronic surveillance and pen register and trap and trace court orders have been frustrated or were not sought, in whole or in part, because of various technological impediments (id. at 24, 37).

19. Director Freeh noted that this problem was becoming quite serious for the public safety because "the nation's telecommunications networks are routinely used in the commission of serious criminal activities, including terrorism and espionage. Organized crime groups and drug trafficking organizations, which are often highly structured, rely heavily upon telecommunications to plan and execute their criminal activities and hide their illegal proceeds" (id. at 16). Accord id. at 6, 7-8.

20. The changes in the telecommunications industry have had such a great impact on law enforcement because, as Director Freeh explained, court-authorized electronic surveillance is "one of its most important investigative techniques — if not the most important. Use of the technique has been critical in fighting organized crime, drug trafficking, public corruption, fraud, terrorism, and violent crime, and in saving numerous innocent lives. In many of these cases, the criminal activity under investigation could never have been fully detected, prevented, adequately investigated, or successfully prosecuted without the use of evidence derived from court-ordered electronic surveillance" (id. at 17). Accord id. at 6, 8.

21. For example, Director Freeh described how electronic surveillance had allowed the FBI to intercept conversations in which Mafia members planned three murders, two of which the Bureau was able to prevent. And, court-ordered electronic surveillance allowed FBI agents and police officers in 1990, to learn about and stop a planned "shoot out" between rival Asian gangs in New York. Further, in 1990, relying heavily upon electronic surveillance, the FBI thwarted two individuals conspiring to abduct, torture, and kill a teenage boy for a "snuff murder" film. Id. at 20-21. Director Freeh also noted instances in which electronic surveillance helped solve outstanding criminal investigations, including one in 1991 of the murder of a United States court of appeals judge. Id. at 20-21.

22. Director Freeh pointed out to Congress how the Federal Government had been attempting since 1992 to work with telecommunications industry personnel at all levels to resolve the problems being caused for law enforcement agencies by the changes in the industry. The Government learned through these discussions that the needs of law enforcement were not being incorporated into carriers' system requirements, and several industry executives made clear that these needs would be met only if there were legislation so requiring. Id. at 25. The Government therefore began a legislative initiative in 1992, but met with industry resistance. Discussions between law enforcement agencies and industry officials continued, and industry representatives "recognize[d] the problems and impediments that [new] telecommunications technologies are creating for law enforcement" (id. at 26). Eventually, the Federal Government determined that comprehensive legislation was needed, and the Clinton Administration therefore proposed a bill in 1994.

23. Director Freeh explained that the purpose of the Administration's legislative initiative was "to maintain technological capabilities commensurate with existing statutory authority — that is, to prevent advanced telecommunications technology from repealing *de facto* the statutory authority already conferred by the Congress" (id. at 27) to carry out electronic surveillance. "With court approval, law enforcement is now technically able to wiretap on the old technology. We simply seek to ensure a failsafe way for law enforcement to conduct court-authorized wiretapping on the recently deployed and emerging technology" (id. at 6).

24. When legislation was initially proposed, there was concern that the Administration had not sufficiently demonstrated the existence of a problem. Therefore, the FBI conducted a new survey of federal, state, and local law enforcement officials, and presented further evidence to committees from both Houses of Congress in April 1994. See H.R. Rep. No. 103-827, 103d Cong., 2d Sess. 14-15 (1994), reprinted at 1994 U.S. Code Cong. & Admin. News (USCCAN) 3489 (cited hereafter as "House Report"). Following receipt of these data, "representatives of the telecommunications industry * * * acknowledge[d] that there will be increasingly serious problems for law enforcement interception posed by new technologies and the new competitive telecommunications market." Id. at 15; accord, 140 Cong. Rec. H10782 (Oct. 4, 1994) (Rep. Edwards) (the FBI "did their homework, and they proved there is a problem"); FCC Notice at 9-10 ("Call forwarding, three-way conferencing, voice recognition calling, digital features, and cellular services were specifically identified as making electronic surveillance difficult or impossible to conduct").

25. Following further hearings in August and September 1994, a bill "to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes" (House Report at 1) was favorably reported in both Houses of Congress.[3] The bill was passed by Congress and signed into law by the President as the Communications Assistance for Law Enforcement Act (CALEA) on October 25, 1994. Pub. L. No. 103-414, 108 Stat. 4279 (1994).

26. The Judiciary Committees in the House of Representatives and the Senate explained that the purpose of CALEA "is to preserve the government's ability pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services." House Report at 9. Congress made clear that it intended to pay carriers for their reasonable costs incurred in modifying existing equipment to comply with new capability requirements, and for expansions in capacity to accommodate law enforcement needs. Id. at 10.

27. The Congressional reports on CALEA recognize the problems described by Director Freeh and others and the need for federal legislation to impose a requirement of cooperation on the telecommunications industry. House Report at 10-16; see also 140 Cong. Rec. H10782 (Oct. 4,

[3] Because joint Senate and House hearings on this proposed legislation were held, the Senate report on the legislation (S. Rep. No. 103-402, 103d Cong., 2d Sess. (1994)) is very similar to the House report. For simplicity, in this petition we cite only to the House report.

1994) (Rep. Oxley) ("Currently, the telecommunications industry is undertaking revolutionary changes in its technology, changes that could make it impossible for police agencies to execute lawful court orders. In some instances, cellular technology and new digital features have already frustrated court ordered wiretaps").

28. To meet this need, Congress designed CALEA to "require[] telecommunications common carriers to ensure that new technologies and services do not hinder law enforcement access to the communications of a subscriber who is the subject of a court order authorizing electronic surveillance. The bill will preserve the government's ability, pursuant to court order, to intercept communications that utilize advanced technologies such as digital or wireless transmission." House Report at 16. Congress made clear that its intent in imposing assistance requirements on telecommunications common carriers was "to preserve the status quo." House Report at 22.[4] CALEA was intended to "allow the FBI and Federal law enforcement to follow the exact same laws we have today and the same rules we have today, to be able to conduct wiretaps in kidnaping cases, national security cases and others." 140 Cong. Rec. S13999 (Oct. 4, 1994) (Sen. Leahy); accord FCC Notice at 9 ("Congress passed CALEA to preserve the ability of law enforcement officials to conduct

---

[4] The House report stated that in preserving the ability of law enforcement agencies to continue to conduct effective electronic surveillance, "[t]he Committee intends the assistance requirements in section 2602 to be both a floor and a ceiling" and that it "expects industry, law enforcement and the FCC to narrowly interpret the requirements" (id at 22-23). Thus, Congress did not want the Commission to expand the requirements legislatively imposed through CALEA. As we describe in the discussion section of this petition, the capabilities being sought by law enforcement are those required by CALEA's language, and thus fit within a "narrow" interpretation of the statute's requirements.

authorized electronic surveillance in the face of the recent, rapid, technological changes in telecommunications that threaten their ability to intercept communications").

29. At the same time that Congress was compelling telecommunications carriers to assist law enforcement in carrying out electronic surveillance successfully, it intended CALEA to provide further privacy protections for specified types of communications,[5] and to ensure that compliance with the requirements of law enforcement would not impede the development and deployment of new technologies and customer services. House Report at 17-19. In addition, "[t]he legislation gives industry, in consultation with law enforcement and subject to review by the FCC, a key role in developing the technical requirements and standards that will allow implementation of the requirements." House Report at 22-23.

30. For purposes of this petition, the central part of CALEA is Section 103(a) (47 U.S.C. § 1002(a)), which mandates that telecommunications carriers "shall ensure" that their equipment, facilities, or services are capable of expeditiously isolating and delivering intercepted communications and call-identifying information to law enforcement agencies. See FCC Notice at 10-11 ("While carriers have been required since 1970 to cooperate with law enforcement officials' efforts to conduct court-authorized electronic surveillance (see 18 U.S.C. § 2518(4)), the question

[5] Among other matters, Congress added privacy protections by limiting the nature of the data that can be obtained through pen registers and certain other types of surveillance, changing the nature of the order needed to obtain electronic mail addresses and communications, extending privacy protections to cordless telephones and certain data communications transmitted by radio, and stating explicitly that the statute does not limit the rights of subscribers to use encryption. See House Report at 17-18.

of whether carriers have an affirmative obligation to design or modify their systems to accommodate such surveillance has never been adjudicated. CALEA for the first time imposes such an affirmative obligation upon telecommunications carriers" (footnote omitted)).

31. Under Section 103(a) (47 U.S.C. § 1002(a)), each telecommunications carrier "shall ensure" that its "equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications" are "capable of":

> (1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government;
>
> (2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier--
>
> > (A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and
> >
> > (B) in a manner that allows it to be associated with the communication to which it pertains,
>
> except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices, * * * such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number);
>
> (3) delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and

(4) facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects--

(A) the privacy and security of communications and call-identifying information not authorized to be intercepted: and

(B) information regarding the government's interception of communications and access to call-identifying information.

32. CALEA thus does not expand law enforcement agencies' power or authority to conduct electronic surveillance; that authority continues to be defined principally by Title III. CALEA was instead designed to enable law enforcement agencies to keep pace with rapidly changing telecommunications technologies by preserving law enforcement officers' access to all communications authorized to be intercepted and by making available the same kinds of information about a subscriber's services and their use that has always been available to law enforcement officers. At the same time. CALEA protects important privacy interests of legitimate telephone users.

C. Post-Enactment Developments

33. Congress recognized that implementation of the assistance capability requirements in Section 103 would require a cooperative effort between law enforcement and industry. Therefore. Section 107(a)(1) of CALEA (47 U.S.C. § 1006(a)(1)) provided for the Attorney General to "consult" with appropriate standard-setting organizations of the telecommunications industry and other interested groups "[t]o ensure the efficient and industry-wide implementation of the assistance capability requirements."

34. Immediately after CALEA was enacted, the FBI engaged in extensive discussions with telecommunications industry representatives. In May 1995, a subcommittee of the industry TIA Standards Committee (Subcommittee TR45.2) began discussing the development of a standard electronic surveillance scheme to meet the CALEA requirements. Based on these discussions, and in response to industry requests for detailed technical specifications of its requirements, the FBI in 1996 published its Electronic Surveillance Interface Document, setting forth recommended technical specifications to meet the assistance capability requirements it believed to be required by Section 103 of CALEA.[6]

35. The FBI maintained that any CALEA-based standard should require telecommunications carriers to provide, in addition to other basic functions, a number of specific assistance capabilities. Among other things, the FBI sought provisions that would provide:

> -- Access to the communications of all parties in a conference call supported by the subscriber's service or facilities;
>
> -- Access to all subject-initiated dialing and signaling activity;
>
> -- Information indicating whether a party is connected to a multi-party call at any given time ("party hold," "party join," and "party drop" messages);
>
> -- Notification messages for in-band and out-of-band signaling;
>
> -- Timely delivery of call-identifying information;
>
> -- Automated reporting of surveillance status;
>
> -- Delivery of all call-identifying information over call data channels; and

---

[6] See Electronic Surveillance Interface Document, Issue 1.0, Federal Bureau of Investigation (June 24, 1996), attached hereto as Appendix 2.

-- A limited number of standardized delivery interfaces.

These provisions are discussed below and described more fully in Law Enforcement Ballot Comments to SP-3580 A (October 28, 1997), attached hereto as Appendix 3. The FBI sought these provisions in order to provide law enforcement agencies with essentially the same type of information they have historically been able to acquire so that they can continue to conduct electronic surveillance effectively in a carrier-controlled, switch-based or network-based surveillance environment.

36. In February 1997, TIA Subcommittee TR45.2 released its Lawfully Authorized Electronic Surveillance (LAES) standards document ("SP-3580") and put it to ballot. The SP-3580 proposed standard did not address any of the capabilities and provisions listed above. A number of law enforcement agencies, believing that SP-3580 was inadequate because it did not address these essential electronic surveillance capabilities, voted against adoption of the document. In addition, the law enforcement community submitted extensive ballot comments identifying the deficiencies of SP-3580. TIA then submitted a revised standard, called SP-3580A, which law enforcement representatives again opposed because it did not include the referenced capabilities. In July 1997, over the objection of law enforcement representatives, TIA established a parallel track in which an identical standards document, still without the referenced capabilities, was renamed as document PN4116 and sent to ballot as proposed interim standard TIA/EIA/IS-J-STD-025 ("J-STD-025"). Only industry votes were counted, even though all submissions, including 184 opposing submissions from the law enforcement community, ostensibly were "considered" by TIA Subcommittee TR45.2.

37. On December 8, 1997, TIA adopted J-STD-025 as an interim standard.[7] The interim standard fails to include any of the electronic surveillance capability requirements described above. After careful review, the Department of Justice has determined that the failure of the interim standard to include these provisions renders it deficient as a means of carrying out Section 103 of CALEA and the Congressional purposes underlying CALEA.[8]

38. Congress anticipated that standards adopted by industry might prove inadequate to carry out Section 103. Section 107(b) of CALEA therefore provides for any government agency (or other person) that believes an industry standard to be deficient to petition the Commission to establish, by rule, technical requirements and standards. Section 107(b) authorizes the Commission to establish technical requirements and standards that: (1) "meet the assistance capability requirements of section 103 by cost-effective methods"; (2) "protect the privacy and security of communications not authorized to be intercepted"; (3) "minimize the cost of such compliance on residential ratepayers"; (4) "serve the policy of the United States to encourage the provision of new technologies and services to the public"; and (5) "provide a reasonable time and conditions for compliance with and the transition to any new standard * * * ." 47 U.S.C. § 1006(b)(1).

---

[7] The title page and table of contents of J-STD-025 are attached hereto as Appendix 4 with permission from TIA. TIA has forwarded a document identical in substance to J-STD-025, denominated TIA SP3580A, to the American National Standards Institute for adoption as a national standard.

[8] See Letter of February 3, 1998 from Stephen R. Colgate, Assistant Attorney General, to Mr. Tom Barba, Steptoe & Johnson, attached hereto as Appendix 5.

39. The Attorney General and other Department of Justice officials have continued meeting with telecommunications industry representatives over the past few months in an effort to persuade industry that the interim standard fails to meet the requirements of CALEA and to arrive at standards that satisfy those requirements. However, these discussions have proven unsuccessful. Consequently, the Department of Justice and the FBI are filing this petition to invoke the authority and assistance of the Commission in an expedited rulemaking proceeding.

III. DISCUSSION

A. THE COMMISSION SHOULD ESTABLISH TECHNICAL REQUIREMENTS AND STANDARDS THAT MEET THE REQUIREMENTS OF CALEA

1. The Commission Has the Authority To Entertain This Petition and Grant the Relief Requested

40. As noted above, Section 107(b) of CALEA (47 U.S.C. § 1006(b)) vests the Commission with the authority to issue a rule establishing technical requirements or standards that meet the assistance capability requirements of Section 103 of CALEA. A government agency may petition for such a rule if it believes that a "publicly available technical requirement or standard adopted by an industry association or standard-setting organization" under Section 107(a)(2) of CALEA is deficient. In this case, the TIA interim standard is a "publicly available technical requirement or standard adopted by an industry association or standard-setting organization * * * to meet the requirements of section 103," and the Department of Justice and the FBI have concluded, for reasons discussed below, that the interim standard is deficient in significant respects. The Commission therefore has the authority under Section 107(b) to entertain this petition and establish appropriate technical requirements or

standards by rule. See FCC Notice at 65 ("The Commission may * * * establish technical standards or requirements * * * if a government agency or any other person believes that any standards issued [by industry] are deficient.").

41. The Commission is also authorized to issue a rule in this proceeding by Sections 4(i) and 229(a) of the Communications Act of 1934 (47 U.S.C. §§ 154(i) and 229(a)). Section 4(i) gives the Commission the general authority to "make such rules and regulations, and issue such orders, not inconsistent with [the Act], as may be necessary in the execution of its functions." 47 U.S.C. § 154(i). Section 229(a), which was added to the Communications Act by Section 301 of CALEA (108 Stat. 4292-93), specifically provides that "[t]he Commission shall prescribe such rules as are necessary to implement the requirements of" CALEA. Id. § 229(a). The authority conferred on the Commission by Section 4(i) and Section 229(a) of the Communications Act complements the authority conferred by Section 107(b) of CALEA.[9]

2. Action by the Commission Is Needed To Correct the Deficiencies of the TIA Interim Standard and Meet the Requirements of CALEA

42. Congress enacted CALEA "to preserve the ability of law enforcement officials to conduct authorized electronic surveillance in the face of the recent, rapid technological changes in

---

[9] Section 1.401(a) of the Commission's rules (47 C.F.R. § 1.401(a)) provides that "[a]ny interested person may petition for the issuance, amendment or repeal of a rule or regulation." The Department of Justice, the FBI, and other members of law enforcement are "interested persons" within the meaning of Section 1.401(a).

telecommunications that threaten their ability to intercept communications." FCC Notice at 9. For reasons set forth below and in the attachments to this petition, the TIA interim standard is not adequate to meet this statutory mandate. If the deficiencies in the interim standard are not cured, the ability of federal, state, and local law enforcement agencies to carry out lawfully authorized electronic surveillance will be seriously impaired, to the significant harm of public safety and law enforcement. The Commission therefore should reject the interim standard with additional technical requirements and standards that meet the requirements of CALEA.

43. This petition identifies a number of provisions that are missing from the interim standard and that should be included in technical standards established by the Commission. Each of these provisions is set forth in Appendix 1 to this petition (see Appendix 1). Adoption of the provisions of the interim standard, "meet the assistance capability requirements of section 103 by cost-effective methods" (47 U.S.C. § 1006(b)(1)), and satisfy the requirements of (47 U.S.C. § 1006(b)(2)-(5)).

44. In the discussion that follows, we address the [illegible] and explain the corresponding provisions of the proposed rule [illegible] relates to one or more capabilities that are missing from the [illegible] met under Section 103. In some instances, the capability [illegible] can be implemented only in one way, and the provisions [illegible] means of satisfying the capability in question. In other instances, [illegible] capabilities

missing from the interim standard could be implemented in more than one way. In those instances, the provisions of the proposed rule are intended to represent the most effective means (although not necessarily the only means) by which the capability can be carried out.

45. In many respects, the provisions of the proposed rule concern communications and call-identifying information that law enforcement historically has received. In other respects, which are noted specifically below, the provisions of the proposed rule will result in the delivery of call content and call-identifying information that law enforcement has not previously received, either because law enforcement was technically impeded from accessing the services or because the services were not available to the subscribers in the past. By its terms, Section 103 of CALEA obligates carriers to provide law enforcement with "all wire and electronic communications * * * to or from equipment, facilities, or services of a subscriber" and "call-identifying information that is reasonably available to the carrier"; Section 103 does not restrict this obligation to those communications and call-identifying information that were accessible to law enforcement in the pre-digital era. More generally, the language and legislative history of CALEA make clear that Congress intended for the electronic surveillance capabilities of law enforcement to keep pace with technological developments in the telecommunications industry. As technological changes have made possible new communications services, new information is generated regarding the use of such services by subscribers. Law enforcement cannot preserve the status quo in a meaningful sense unless it is able to obtain such information and thereby keep pace with the evolution of services and technologies. Moreover, all of the call content and call-identifying information at issue in this petition can lawfully be acquired by law enforcement pursuant to Title III surveillance orders and pen register orders, and

the failure to adopt the proposed requirements and standards will thus result in the inability of law enforcement to obtain information that it is legally entitled to acquire.

46. **(a)** Ability to intercept the communications of all parties in a conference call supported by the subscriber's service or facilities. Under Section 103(a)(1) of CALEA, telecommunications carriers are obligated to ensure that their equipment, facilities, and services are capable of "expeditiously isolating and enabling the government * * * to intercept * * * all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier * * * ." 47 U.S.C. § 1002(a)(1) (emphasis added). The TIA interim standard does not satisfy this requirement because it does not ensure the ability of law enforcement to intercept all of the communications of all parties in a conference call supported by the subscriber's service or facilities.

47. At the outset, we wish to be clear about the meaning of several terms used in our discussion of this issue and related issues in this petition. When we refer to "subscriber," we are referring to the person or entity whose "equipment, facilities, or services" (47 U.S.C. § 1002(a)) are the subject of an authorized law enforcement surveillance activity. The subscriber often will be a person or entity suspected of criminal activity, but in some instances, the subscriber will simply be someone whose relationship to a suspected criminal (e.g., spouse or employer) makes it likely that criminal activity will be transacted or discussed over the subscriber's facilities. When we refer to "intercept subject" or "subject," we are referring to any person who is using the subscriber's equipment, facilities, or services, and whose conversations (or dialing activity) therefore would be capable of

being acquired during an interception. In a particular investigation, the "intercept subjects" could include the subscriber, who may or may not be involved in criminal activity; a non-subscriber who is not involved in criminal activity; or a non-subscriber who is involved in criminal activity. As explained below, to the extent that innocent persons are intercept subjects, their interests are protected by Title III's minimization requirements.

48. Title III does not require the subscriber to be "on the line" in order for law enforcement lawfully to intercept communications taking place over the subscriber's facilities or supported by the subscriber's service. With the exception of "roving wiretaps" (see 18 U.S.C. § 2518(11)), interception orders under Title III are directed at particular telecommunications facilities, not at the subscriber, who may not even be a target of the investigation. An interception order must specify "the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted." 18 U.S.C. § 2518(4)(b); see also id. § 2518(1)(B)(ii).[10] But the government is not required to show that the subscriber whose facilities are to be monitored is involved in any way with the criminal activity at issue. Instead, the government need only show probable cause to believe that the facilities "are being used, or are about to be used, in connection with the commission

---

[10] Although Congress did not define "facility," it is used throughout Title III to describe the thing to be searched, or the communications pathway where the communications are to be intercepted. In practice, the facility is described by the subscriber's telephone number, which would entail network facilities that support and are identifiable with the service associated with that telephone number. It is commonly accepted within the telecommunications industry that "facility" includes numerous components within the entire transmission path over which a communication travels from one conversing party to another. For example, "Facility" is defined as the "[t]ransmission path between two or more points provided by a common carrier." North American Telecommunications Association, INDUSTRY BASICS (4th ed.).

of [the specified] offense, or are leased to, listed in the name of, or commonly used by" the intercept target(s). Id. § 2518(3)(d) (emphasis added). With some frequency, Title III orders are issued for facilities of a subscriber who has some connection with a person suspected of criminal activity but who has no involvement in the criminality himself (e.g., an employer, neighbor, or relative).

49. Neither does Title III confine the government to communications in which the individual under investigation is taking part. When the government executes an interception order, it may intercept any communications carried over the facilities covered by the order that relate to the criminal activity under investigation and are otherwise within the scope of the order, even if the individual under investigation does not participate in such communications. See United States v. Kahn, 415 U.S. 143 (1974); see also 18 U.S.C. § 2518(4)(a) (interception order need not specify the identities of the persons whose communications are to be intercepted if the identities are not known). The government is, of course, obligated to "minimize the interception of communications not otherwise subject to interception" under Title III. 18 U.S.C. § 2518(5).[11] But this minimization obligation means only that the government must minimize the interception of communications that are unrelated to criminal activity; it does not mean that the government is foreclosed from intercepting communications that do involve criminal activity merely because they do not involve a particular investigatory target.

---

[11] Minimization is ordinarily effected by manually discontinuing the interception and recording of conversations when criminal conduct is not being discussed.

50. In the context of traditional two-party "plain old telephone service" (POTS), telecommunications historically have been accessible at any place within the local loop associated with a call. Thus, any communication that could be "tagged" or identified as connected to a particular subscriber's telephone service would be technically subject to interception, regardless of who is being intercepted over that service.

51. POTS is being replaced by telephone services with greater functionality, including conference calling capabilities, which allow a subscriber (or other person using the subscriber's services) to join several different parties, each on a separate "leg" of the call, in one call. Title III interception orders authorize law enforcement to acquire all criminal communications of all parties conversing over the subscriber's facilities or services, including communications on any "leg" of a conference call at all times. Under the TIA interim standard, however, law enforcement would be able to intercept only those communications occurring over the leg of the call to which the subscriber's terminal equipment is actually connected to each leg of the call at any point in time. As long as the subscriber's terminal equipment is connected, law enforcement could monitor all legs of the call. But law enforcement would have no access to certain communications supported by the subscriber's service or carried over the subscriber's facilities in the event that the person using the subscriber's services placed some of the conferenced parties on hold or dropped off the call. This does not amount to a reduction in the information that has been available to law enforcement under POTS, but as we show below, it nevertheless falls short of carrying out the legal obligations imposed by Section 103 of CALEA.